TDB-ACC-NO: NN9603363

DISCLOSURE TITLE: Anonymous Delivery of Goods in Electronic Commerce

PUBLICATION-DATA: IBM Technical Disclosure Bulletin, March 1996, US

VOLUME NUMBER: 39

ISSUE NUMBER: 3

PAGE NUMBER: 363 - 366

PUBLICATION-DATE: March 1, 1996 (19960301)

CROSS REFERENCE: 0018-8689-39-3-363

DISCLOSURE TEXT:

Disclosed is a method that allows on-line (electronic) purchase and delivery of (both electronic and physical) goods in a manner that preserves anonymity of the consumer. The method is secure and resistant to cheating by both consumers and merchants.

The following notation is used throughout this document.

C,M - Consumer and Merchant, the protocol participants;
ID-x - user ID of X;
PK-x - Public Key of X (X=C or X=M);
SK-x - Secret/Private Key of X (X=C or X=M);
Rc/Rd - Random numbers (nonces)
Cert-x - Public Key Certificate of X; includes PK-x
H(text) - Strong one-way Hash function computed over "text", e.g., Secure Hash Function (SHA) or MD5.
Sx(text)- Signature computed under SKx, Sx text =SK-x(H(text))
[text] - Optional text

Prerequisites for the present method are the possibility of anonymous communication (e.g., (1) and a public key infrastructure (for merchants only). The buying process is started by a sender, usually a prospective consumer, who composes an offer request with a plaintext (unencrypted) description of the desired product or service and a random quantity H(Rc). This construction does not by itself

reveal the sender's identity.

The resultant offer request is sent anonymously to one or more selected merchant(s), or even broadcasted, via the network. If a merchant decides to make an offer, he/she composes a reply with an offer description and his/her digital signature (SIG_offer), which is computed over the sender's random quantity H(Rc), and transmits it back to the sender. The merchant's public key may also have to be transmitted since in some cases the sender does not yet have it.

Upon receiving the message, the consumer can (if necessary) extract the merchant's public key and verify the merchant's SIG_offer computed over (among other values) the consumer's H(Rc).

The present method commences when the consumer decides to purchase the aforementioned merchandise based on a previous bid/offer. The payment process itself is outside the scope of this document. (See (2) or (3) for examples of secure electronic payment protocols and scenarios.)

Assume that the payment process takes place before the delivery of goods (although it can, in principle, take place concurrently.)

Step 1.

a) (note: Consumer is assumed to retain Rc and SIG_offer from above.) Consumer generates another random number Rd and computes H(Rd).

b) Optionally, consumer generates a public/private key-pair (PKtmp,SKtmp). (This key-pair is to be used for the delivery of goods later.)

c) Consumer sends to merchant a COMMIT_REQUEST message containing:

H(Rc), H(Rd), C_options

where H(Rc), H(Rd) are as described above and "C_options" are optional parameters including, for example: date/time-stamp, PKtmp, mailing address (for off-line, non-electronic goods), etc.

Step 2.

a) Merchant receives the COMMIT_REQUEST and extracts both H(Rc) and H(Rd). H(Rd) is stored for future reference.

b) Using H(Rc) merchant searches his records and checks if the corresponding bid/offer has been processed. If the offer is no longer valid, merchant sends and error message to consumer and terminates processing.

c) If the offer is still valid, merchant composes and send to consumer a COMMIT message containing:

SKm COMMIT_REQUEST, M_options , M_options
_____ _____/
SIG_commit

where SIG_commit represents a merchant's signature computed with SKm over the specified data. "M_options" are optional parameters.

Step 3.

a) Consumer receives the OFFER message and (using merchant's public key PKm) verifies SIG_commit. If the signature is invalid, an error message to that effect is sent to merchant.

b) If signature is valid, consumer generates and sends to merchant a DELIVERY_REQUEST message containing: Rc

Step 4.

a) Merchant receives DELIVERY_REQUEST and extracts Rc.

b) Merchant computes TMP=H(Rc) and compares to H(Rc) stored in the appropriate transaction record. If there is no match, an error message to that effect is sent to consumer.

c) If TMP matches H(Rc) merchant composes and sends to consumer, a DELIVERY message containing:

GOODS, SKm SIG_commit,GOODS
___ _____/
SIG_deliver

or, if PKtmp was included in COMMIT_REQUEST message (as in Step 1 above), a DELIVERY message contains:

PKtmp(GOODS), SKm SIG_COMMIT,GOODS
\ /
SIG_deliver

where PKtmp(GOODS) denotes the encryption of GOODS under the consumer-generated public key PKtmp.

(Only if PKtmp was included in COMMIT_REQUEST above.)

Step 5.

a) Consumer receives DELIVERY and, if applicable, decrypts PKtmp(GOODS) using SKtmp. (Otherwise, GOODS arrives in the clear.)

b) Using PKm and SIG_commit (received in Step 3) consumer verifies

SIG_deliver. If SIG_deliver is invalid an error message to that effect is sent to merchant.
Otherwise, consumer sends to merchant a TERMINATE message containing Rd.

Step 6.

a) Merchant receives TERMINATE, extracts Rd, computes TMP=H(Rd) and compares it with H(Rd) received in COMMIT_REQUEST (see step 2.) If they match the transaction is terminated. Otherwise, an error message is sent to consumer (perhaps along with the re-transmission of DELIVERY.)

The method presented above provides protection against dishonest behavior by either merchants or consumers involved. Potential cases of cheating and disputes are addressed below. All cases require intervention of a mutually trusted off-line authority that we refer to as COURT.

While dispute resolution is likely to take place off-line, it is expected that consumer will remain anonymous with respect to merchant. However, consumer may be required to reveal his identity to COURT.

At the end of a successful transaction the parties involved must have the following in their possession:

Rc, Rd, SIG_Commit, SIG_offer, H(Rc), H(Rd)

Dispute Scenarios

a) Customer is asked to produce a valid SIG_offer
   a. No valid SIG_offer; merchant prevails.
   b. Valid SIG_offer; continue with (2).

b) Merchant is asked to provide Rc.
   a.

Merchant can not produce the correct Rc; continue with (3).
   b. Correct Rc; continue with (4)

c) Consumer is asked to produce Rc.
   a. Correct Rc; consumer prevails (protocol can be re-run.)
   b. Incorrect or no Rc; merchant prevails.

d) Consumer is asked to produce Rc.
   a. Correct Rc; continue with (5).
   b. Incorrect or no Rc; merchant prevails.

e) Consumer is asked to produce a valid SIG_commit.
a. No valid SIG_commit; merchant prevails.
b. Valid SIG_commit; continue with (6).
f) Merchant is asked to produce Rd.
a. Correct Rd; merchant prevails.

b. Incorrect or no Rd; consumer prevails (merchant is ordered to send a DELIVERY message to consumer and consumer is ordered to reply with a TERMINATE message (the latter containing a valid Rd.)

References

(1) C. Gulcu and G. Tsudik, "Mixing E-mail with BABEL," 1996 Symposium on Network and Distributed System Security (February 1996).
(2) M. Bellare, R. Hauser, A. Herzberg, J. Garay, H. Krawczyk, M. Steiner, G. Tsudik and M. Waidner, "iKP -- A Family of Secure Electronic Payment Protocols," USENIX Conference on Electronic Commerce (July 1995).
(3) D. Chaum, A. Fiat and M. Naor, "Untraceable Electronic Cash," In Proceedings of Crypto'88, Santa Barbara, Ca. (August 1988).

L Number	Hits	Search Text	DB	Time stamp
1	3375	anonymous or anonymity	USPAT	2003/11/03 15:33
2	98	(anonymous or anonymity) same (delivery or delivered)	USPAT	2003/11/03 14:10
3	4	("5724522" | "5812670" | "5815665" | "5890137").PN.	USPAT	2003/11/03 15:14
4	12	6006200.URPN.	USPAT	2003/11/03 15:18
5	1	anonymous adj delivery	IBM_TDB	2003/11/03 15:26
6	20995	anonymous or anonymity	US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/11/03 15:33
7	215	(anonymous or anonymity) same (delivery or delivered)	US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/11/03 15:34
8	82	((anonymous or anonymity) same (delivery or delivered)) and (e or electronic or internet or online or on adj line) near (shop or shopping or buying or purchasing or commerce)	US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2003/11/03 15:35

reviewed all circled

US006006200A

United States Patent [19]

Boies et al.

[11] **Patent Number: 6,006,200**

[45] **Date of Patent: Dec. 21, 1999**

[54] **METHOD OF PROVIDING AN IDENTIFIER FOR TRANSACTIONS**

[75] Inventors: **Stephen Joy Boies**, Mahopac; **Susan Lynn Spraragen**, Ossining, both of N.Y.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

[21] Appl. No.: **09/084,267**

[22] Filed: **May 22, 1998**

[51] **Int. Cl.**[6] **G06F 17/60**

[52] **U.S. Cl.** **705/26**

[58] **Field of Search** 705/26

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,724,522	3/1998	Kagami et al.	705/26
5,812,670	9/1998	Micali	380/25
5,815,665	9/1998	Teper et al.	705/26
5,890,137	3/1999	Koreeda	705/26

OTHER PUBLICATIONS

Sirbu, Marvin A; "Internet Billing Service Design and Implementation", 1993.

Cox, Benjamin T.H.; "Maintaining privacy in Electronic Transactions", Aug. 1994.

Sirbu, Marvin; J.D. Tygar; NetBill: An Internet Commerce System Optimized for Network Delivered Services, Mar. 1995.

Cox, Benjamin; tygar, J.D.; Sirbu, Marvin; NetBill Security and Transaction Protocol, Jul. 1995.

Schneier, Bruce; Applied Cryptography: protocols, algorithms, and source code:, library of congress No. TX–4–216–579, Oct. 1995.

http:/www.ini.cmu.edu/netbill/pubs.html, Apr. 1997.

PC Magazine; vol. 13; No. 18, p. 87; ISSN: 0888–8507; "Needed: A Fee–Based Internet"; Bill Machrone, Oct. 1994.

Information Week; Client–Server; p. 84; "A Standard For Saftery—Net Providers Strive For Encryption and Authentication", Jan. 1995.

Primary Examiner—Allen R. MacDonald

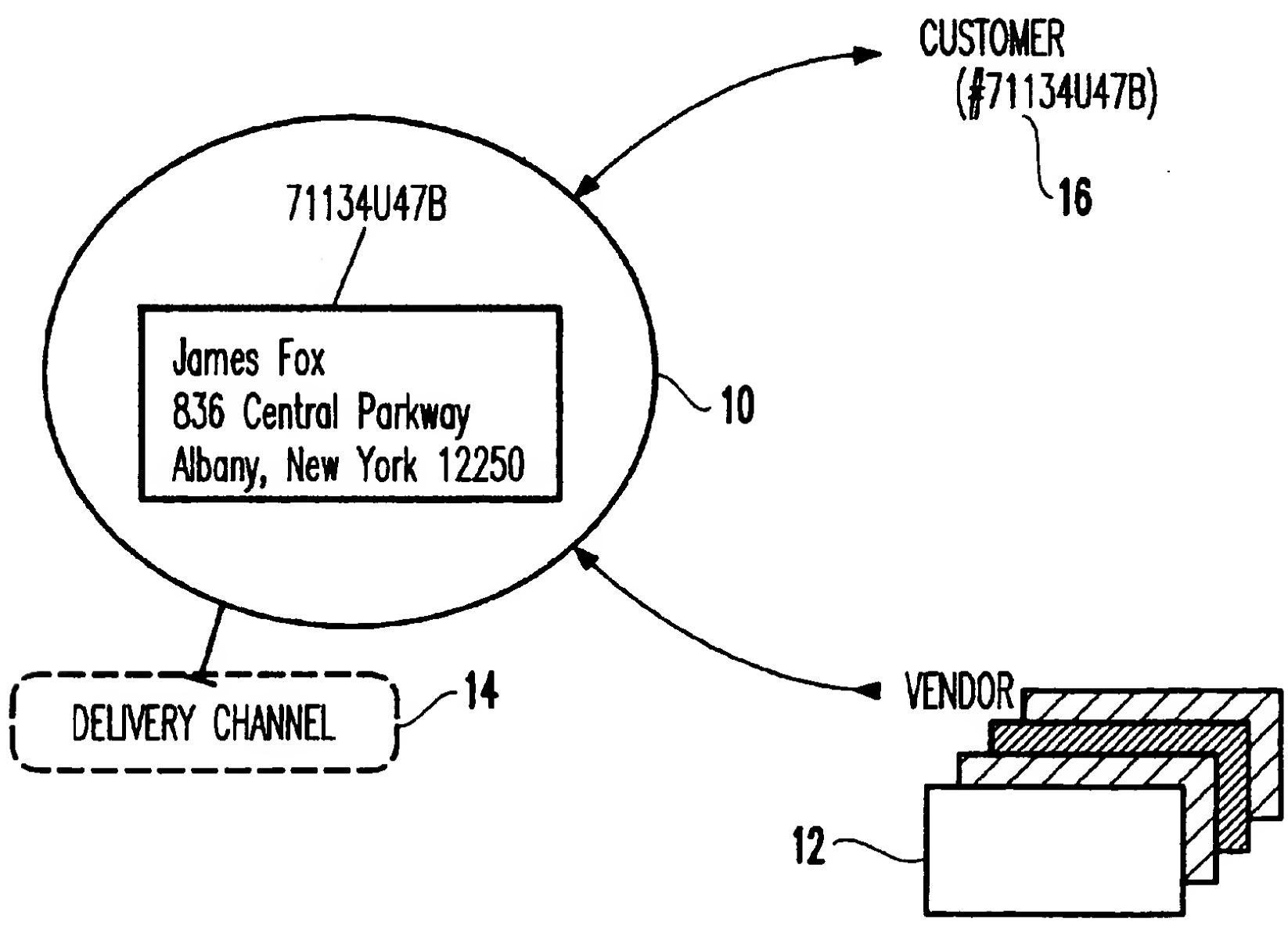
Assistant Examiner—Akiba Robinson-Boyce

Attorney, Agent, or Firm—Whitham, Curtis & Whitham; Stephen C. Kaufman

[57] **ABSTRACT**

Transactions are conducted on the Internet, by telephone or directly with anonymity and privacy. A customer's shipping address is encoded by a multi-digit identifier which is stored in the database of a trusted third party, preferably the shipping company. A user of the system need only identify themselves to a vendor by this multi-digit identifier which prints the identifier in machine readable form on a package delivered to the shipper.

5 Claims, 4 Drawing Sheets



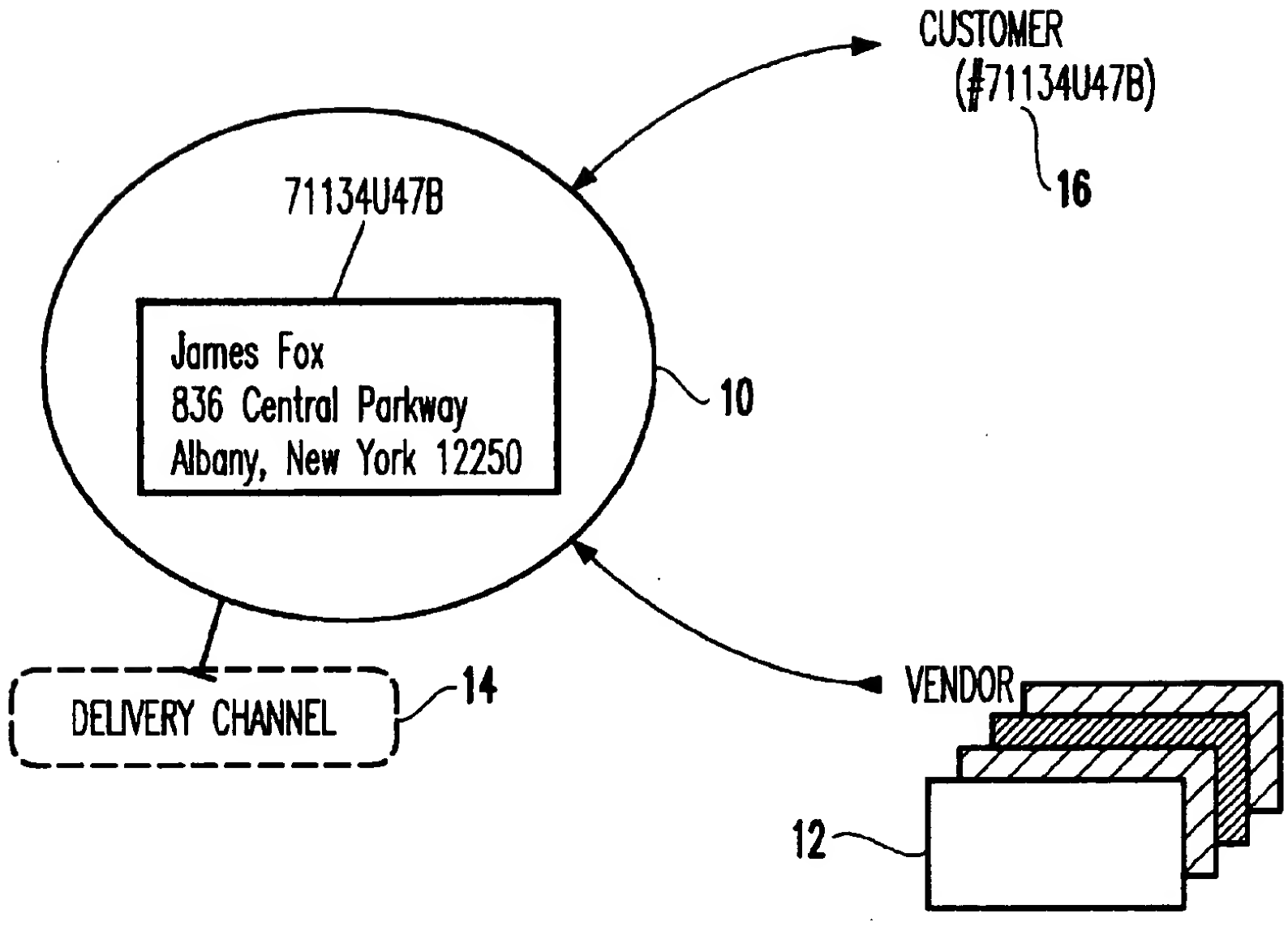

CUSTOMER
(#71134U47B)
16
71134U47B
James Fox
836 Central Parkway
Albany, New York 12250
10
DELIVERY CHANNEL
14
VENDOR
12

FIG.1

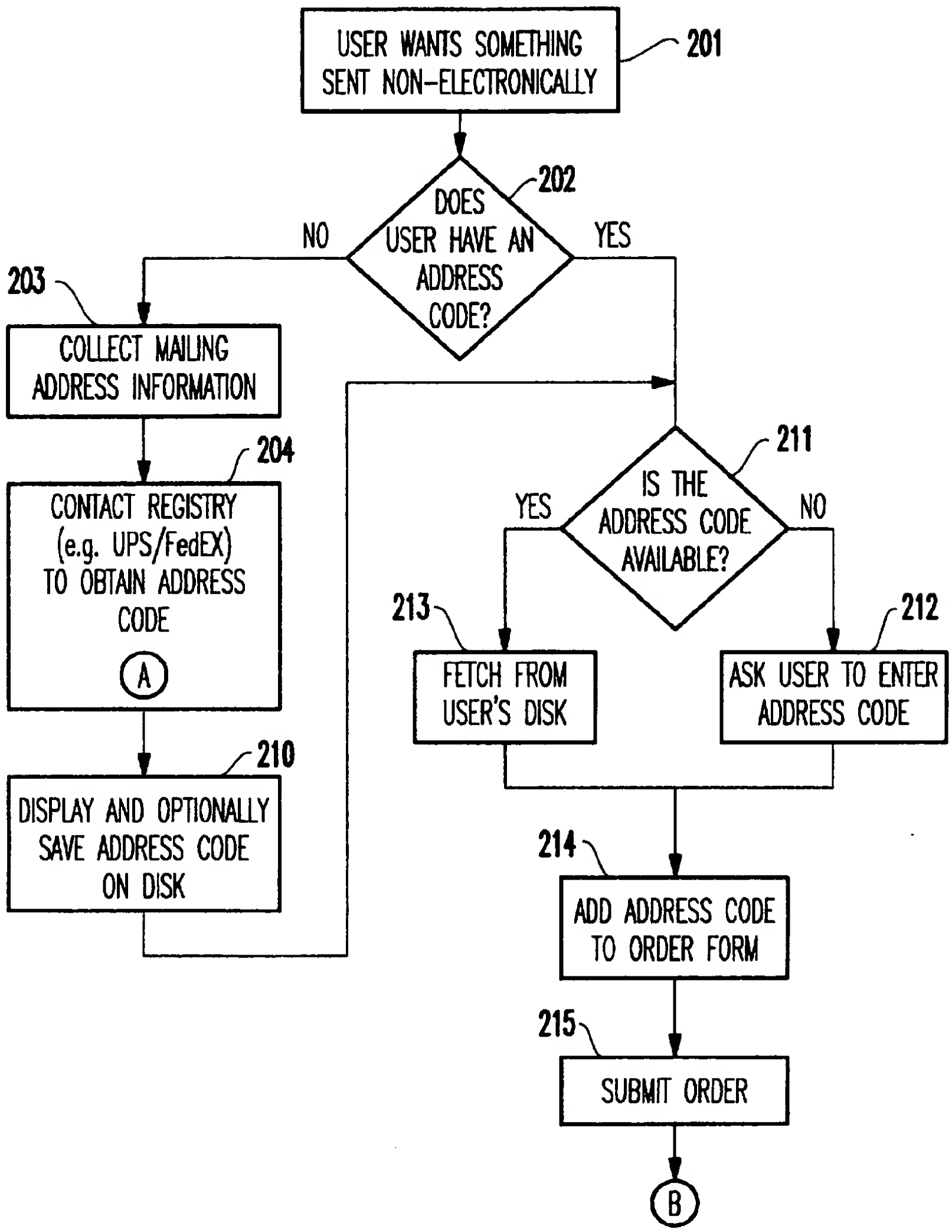

USER WANTS SOMETHING SENT NON-ELECTRONICALLY
201
DOES USER HAVE AN ADDRESS CODE?
202
NO
YES
203
COLLECT MAILING ADDRESS INFORMATION
204
CONTACT REGISTRY (e.g. UPS/FedEX) TO OBTAIN ADDRESS CODE
A
210
DISPLAY AND OPTIONALLY SAVE ADDRESS CODE ON DISK
IS THE ADDRESS CODE AVAILABLE?
211
YES
NO
213
FETCH FROM USER'S DISK
212
ASK USER TO ENTER ADDRESS CODE
214
ADD ADDRESS CODE TO ORDER FORM
215
SUBMIT ORDER
B

FIG.2A

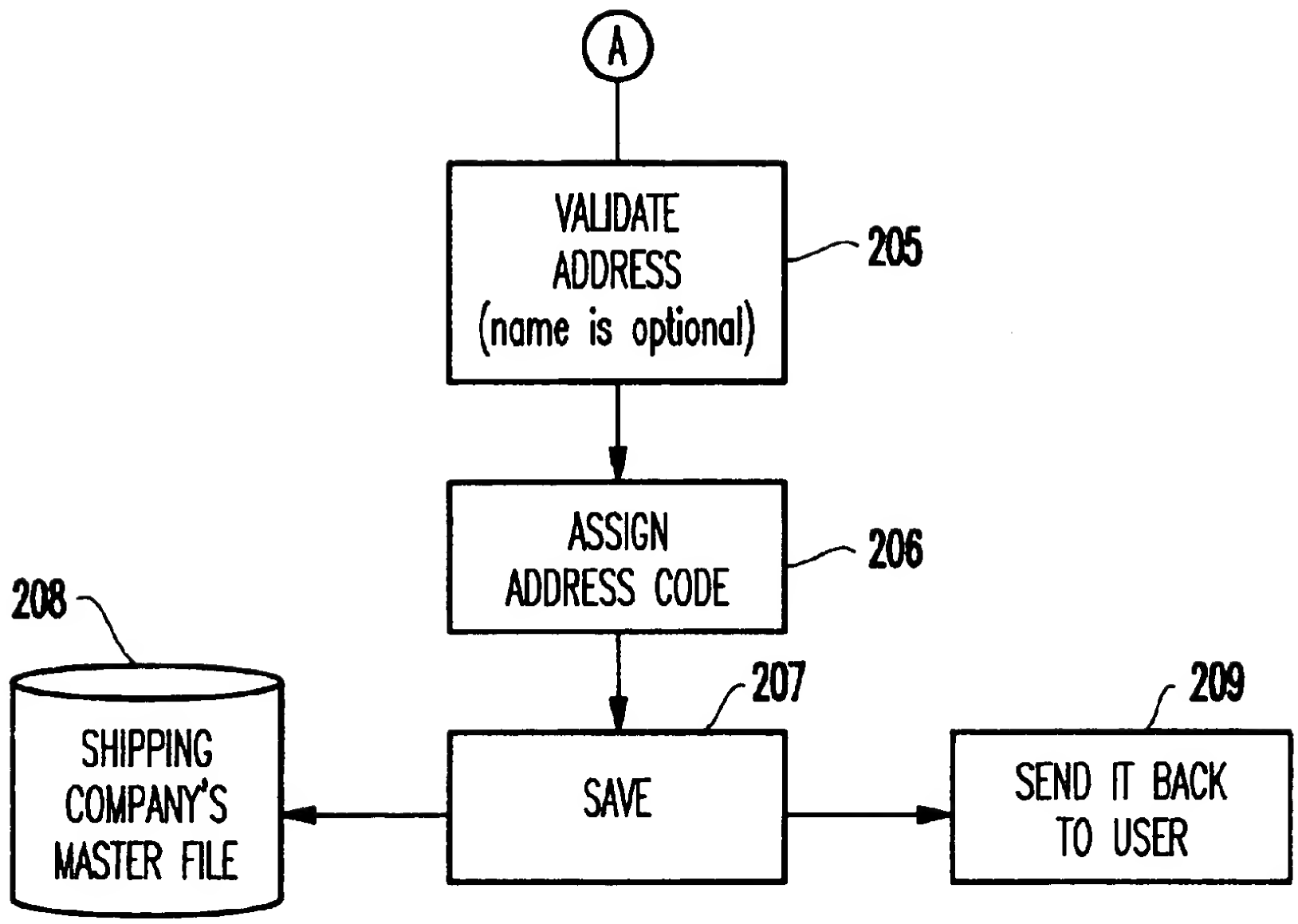


FIG.2B

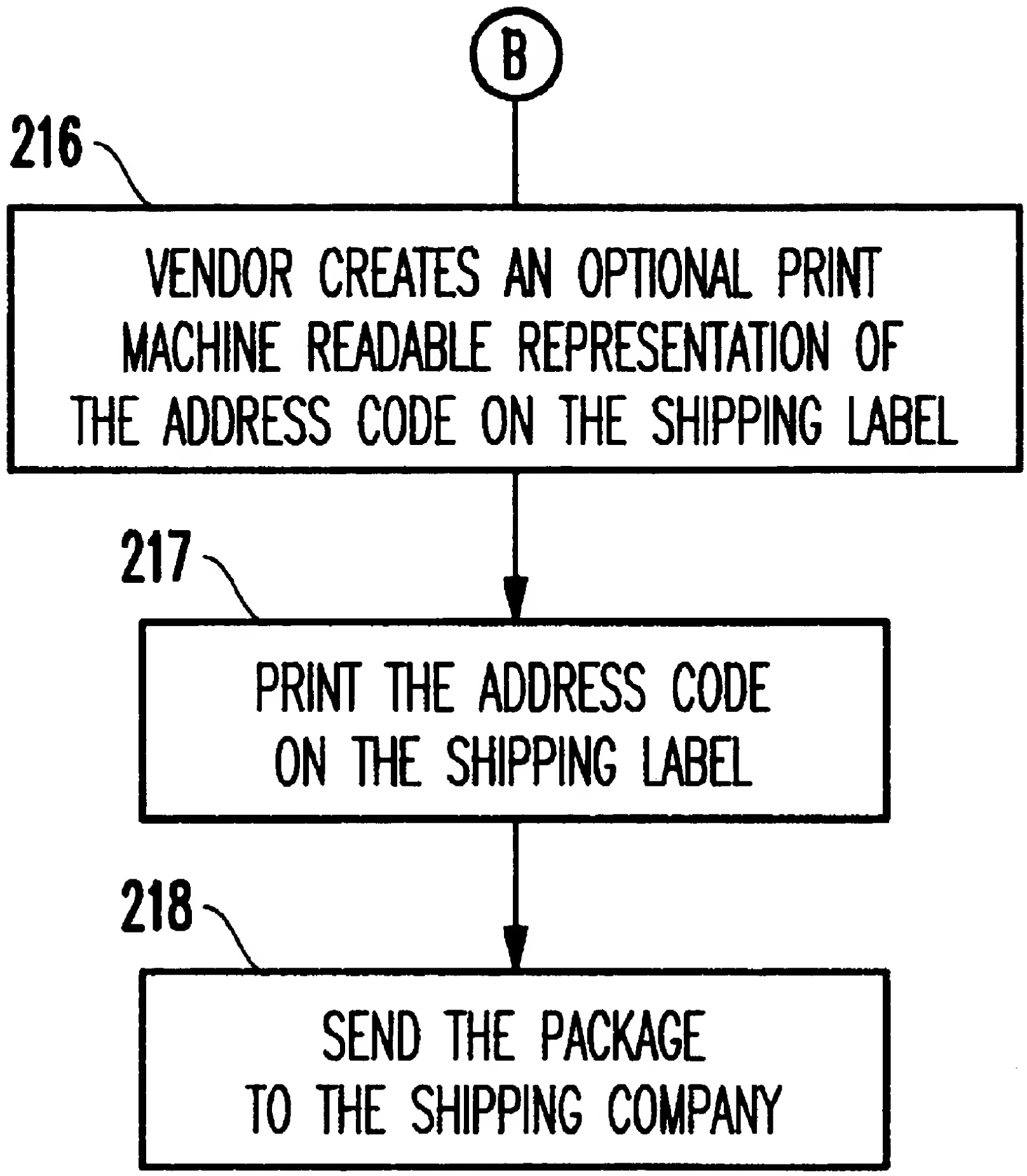


FIG.2C

METHOD OF PROVIDING AN IDENTIFIER FOR TRANSACTIONS

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention generally relates to performing transactions with anonymity and, more particularly, to a method for providing a unique identifier for collectively electronically tagging personal data.

2. Background Description

People are hesitant to supply personal data for making transactions for fear of subsequently being placed on direct marketing mailing lists. This is particularly true in conducting transactions over the Internet. If this step of providing name and address were replaced with a more anonymous identifier, perhaps more potential customers would engage in electronic transactions on the Internet. And for those who do, repeated transactions would be easier as they would only have to provide the one field. Such an anonymous identifier could also be used in other types of transactions as well, including telephone transactions and face-to-face transactions in a retail shop.

In order to accomplish this, however, a third party identifier supplier has to be a trusted part of the transaction. Many transactions requiring name and address information involve having a product shipped to a customer. The provider of that service (e.g., U.S. Postal Service, UPS, Federal Express, or other carrier) could well provide a unique personal identifier for the customer. This same identifier could later be used as an additional means for tracking shipments made to the customer. Rather than using a new delivery identifier for each shipment, the customer could provide their personal identifier to track shipment.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a way to conduct transactions with anonymity and privacy.

According to the invention, there is provided a method for identifying a customer's shipping address by a multi-digit identifier which is stored in the database of a trusted third party, preferably the shipping company. A user of the system need only identify themselves to a vendor by this multi-digit identifier which prints the identifier in machine readable form on a package delivered to the shipper. A further advantage of the invention is that if the customer moves and needs to change their address, they have but one place to do so. Hence, when conducting business with many vendors, one would not need to repeat their address to each vendor for each transaction, rather, all that needs to be provided is an address code.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

FIG. **1** is a schematic diagram showing the creation and use of a personal identifier throughout the course of a transaction according to the invention; and

FIGS. **2A**, **2B** and **2C**, taken together, are a flow chart showing the logic of the system implementing the invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT OF THE INVENTION

Referring now to the drawings, and more particularly to FIG. **1**, there is shown, in s schematic diagram form, the

process of creation and use of a personal identifier for Internet transactions. When ordering a product over the Internet, one must supply to the vendor a shipment address. With this, the vendor can send the product to the customer using some existing delivery mechanism, such as the U.S. Postal Service, UPS, Federal Express, or the like. Also, with this information, the vendor can augment their mailing list and, possibly, sell it to other marketing firms. The purpose of this invention is to conduct the same transactions with anonymity, insuring the privacy of the customer.

The method used in this invention is to employ a third party vendor to supply a unique identifier to the customer that maps to the customer's name and address in a database owned by the third party. The personal identifier is a multi-digit numeric or alphanumeric code assigned to a customer, as indicated at **10**. This code is an accepted field by the vendor **12** that is used for shipping purposes. The shipper **14** is the creator and custodian of the codes. It generates a unique code for each customer, which code is associated with the customer's full shipping address and, optionally, the customer's name, permitting shipment to be made to the customer **16**.

The association is maintained as a private database by the delivery organization. The shipper has an agreement with the customer not to sell its database codes and addresses to outside marketing organizations. The shipper also has an agreement with vendors to use this code with all shipping requests. When the vendor sends a package to the shipper, it is sent with this code for processing.

The process is illustrated in more detail in FIGS. **2A**, **2B** and **2C**, to which reference is now made. A transaction begins at block **201** with the user wanting a product that cannot be sent electronically, i.e., over the Internet. An initial determination is made in decision block **202** as to whether the user has an address code. If not, the mailing address information is collected from the user in function block **203**. Next, in function block **204**, the registry is contacted to obtain an address code. This routine is shown in more detail in FIG. **2B** and begins with validating the address in function block **205**. An address code is assigned in function block **206**, and this code is saved in function block **207** to the shipping company's master file database **208** before a return is made in function block **209** to the main routine in FIG. **2A** where the code is displayed and saved to the user's computer in function block **210**.

Referring again to FIG. **2A**, once the user has an address code then a determination is made in decision block **211** as to whether the address code is available. If not, the user is prompted to enter the address code in function block **212**; otherwise, the code is directly retrieved from the user's hard disk in function block **213**. The address code is added to the order form in function block **214**, and the order is submitted in function block **215**.

Referring now to FIG. **2C**, when the vendor receives the order, the vendor optionally creates a printed, machine readable representation of the address code on the shipping label in function block **216**. The address code is printed to on the shipping label in function block **217**, and the package is sent to the shipping company in function block **218**. The shipping company uses the machine readable address code printed on the shipping label to access the master file **208**. (FIG. **2B**) to retrieve the user'shipping address for delivery of the package.

The benefits to the vendor is that more customers will be more likely to participate in their electronic marketplace if they only need to provide their multi-digit identifier instead

of their name and address. Thus, the vendor does not know their customer's identity, only their preference for one of their products. The benefit for the delivery agent is that the vendors will be more inclined to choose them for delivering packages. The benefit for the customer is that a level of anonymity is established for the transaction.

While the invention has been described in terms of a single preferred embodiment, those skilled in the art will recognize that the invention can be practiced with modification within the spirit and scope of the appended claims.

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

1. A method of conducting transactions while preserving the anonymity and privacy of a user comprising the steps of:

assigning to a user a multi-digit identifier which is stored in a master file database of a trusted third party;

using by a customer the multi-digit identifier to order a product;

printing by a vendor the multi-digit identifier on a package to be delivered to the customer; and

accessing the master file database by a shipper to obtain the customer's shipping address.

2. The method recited in claim 1 wherein the master file database is owned by the shipper.

3. The method recited in claim 1 wherein the multi-digit identifier is printed in machine readable form.

4. The method recited in claim 1 wherein the product is ordered on the Internet.

5. The method recited in claim 1 further comprising notifying by a customer a change of address to the trusted third party in order to effect a change of address.

* * * * *